SARBANES-OXLEY ACT

ASQ Team Says QMS and EMS Standards Support SOX

by **Sandford Liebesman**

In 50 Words Or Less

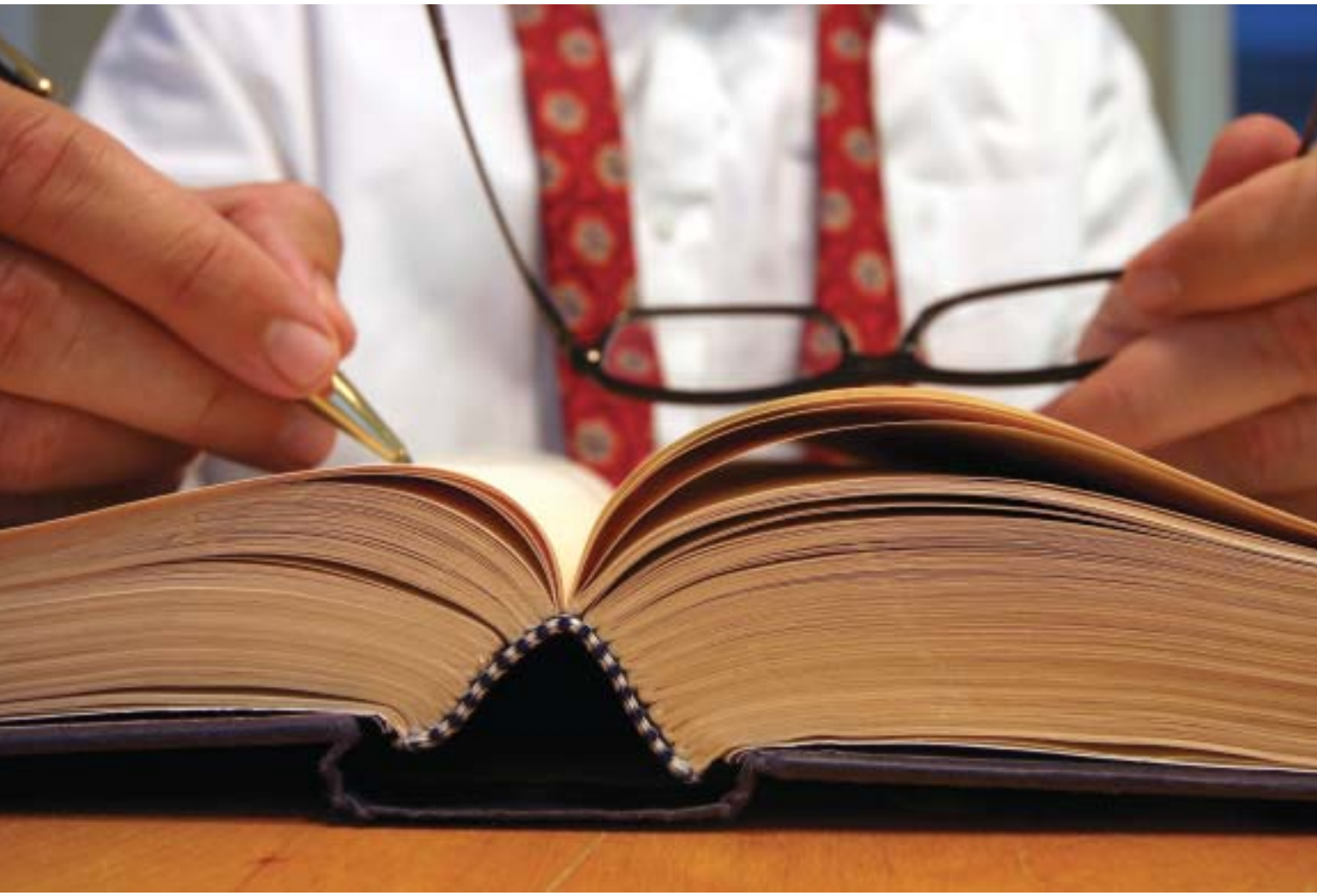
- **The Securities and Exchange Commission and the Public Company Accounting Oversight Board asked for comments on management guidance for internal controls and Sarbanes-Oxley (SOX) auditing standards.**
- **The ASQ SOX Team educated them on how quality and environmental management systems can support the design, management and auditing of SOX.**

The Corporate and Criminal Fraud Accountability Act of 2002, also known as the Sarbanes-Oxley Act (SOX), increases penalties for corporate fraud and imposes greater oversight on accounting firms.[1]

SOX was passed in response to the accounting scandals at Enron, WorldCom, Tyco and other organizations. SOX's goal is to protect investors by improving the accuracy and reliability of corporate disclosures, including quarterly and annual financial reports.

The law's intent was to make the financial system of control more transparent and to reduce the incidence of corporate fraud. Congress expected the law to protect the interests of investors through more appropriate valuation of public company stocks.

The act established the Public Company



Accounting Oversight Board (PCAOB) as a subsidiary of the Securities and Exchange Commission to oversee the auditing and preparation of audit reports by public companies. In 2003, SEC adopted rules requiring stock issuer's annual reports to include an assessment of the company's internal control over financial reporting (ICFR) in addition to an auditor's report on that assessment.

PCAOB's New Auditing Standard

In 2004, the PCAOB created *Auditing Standard No. 2* (AS No. 2) to apply to the newly required external audits.[2]

It soon became evident that compliance to the auditing requirements of the act was very costly, especially for smaller firms. PCAOB and the SEC gathered information from public auditing firms, held two roundtables and received feedback on auditing small businesses.

This information highlighted significant benefits from the focus on corporate governance, but at a significant cost. There was concern that AS No. 2 encouraged auditors to perform procedures not necessary to satisfy the intent of the act.

In response, the PCAOB proposed a new standard,[3] and the SEC proposed a guidance document for management to use in complying with SOX.[4] The PCAOB and SEC asked for public comments by Feb. 26, 2007.

Ron Atkinson, ASQ president at the time, and the ASQ SOX Team each submitted comments on the proposed documents.[5] After receiving the public comments, the PCAOB published the final version of the standard on May 24,[6] and the SEC

published the final version of the guidance document on June 20.[7]

The PCAOB proposal is designed primarily to accomplish the following:

- Focus the audit on a risk based, top-down approach. The auditor should direct testing to the most important controls and emphasize the importance of risk assessment.
- Eliminate unnecessary procedures, such as the requirement to evaluate management's reporting process.
- Allow a reduced number of walkthroughs during audits. Walkthroughs are procedures to evaluate the flow of transactions.
- Permit consideration of knowledge obtained during previous audits and remove barriers to using the work of others.
- Scale the audit for smaller and less complex companies.
- Simplify the requirements by reducing detail and specificity, which should result in better readability and an improved sequential flow of the audit.
- Align the key terms and concepts with those found in the SEC guidance document.
- Discuss fraud risk and antifraud controls at the beginning of the standard to emphasize the importance of these matters in assessing risk.
- Explain the effect entity level controls have on selecting and testing other specific controls. Entity level controls test functions at the top of the organization.

SEC's Interpretive Guidance

The SEC's interpretive guidance for management to use in its evaluation of ICFR as required by section 404 of SOX focuses on conducting a top-down, risk based evaluation and is intended to help companies of all sizes complete their annual evaluations effectively and efficiently. An evaluation that complies with the guidance is one way to satisfy the SEC requirements.

The SEC set two broad principles for conducting the evaluation:

1. Management should evaluate whether it has implemented controls that adequately address the risk that a material misstatement of the financial statements would not be prevented or detected in a timely manner.
2. Management's evaluation of evidence about the operation of its controls should be based on its assessment of risk.

In addition, the guidance relies on general principles rather than being prescriptive. This allows an organization to tailor its responses to their structure and circumstances.

The 2003 SEC rules implementing SOX Section 404 required management to use a framework for evaluating ICFR. The rules do not mandate a specific framework, but they do identify the "Internal Control—Integrated Framework" created by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as an example.[8]

As SOX was implemented, many management teams used the prescriptive AS No. 2 auditing standard instead of COSO. This resulted in duplication and high implementation costs. The SEC guidance is expected to bring organizations back to using COSO.

Comments on AS No. 5 And the Interpretive Guidance

In 2003, four members of ASQ[9] recognized the opportunities for quality management systems (QMSs) and environmental management systems (EMSs) to support the financial managing organizations in satisfying SOX. They formed the ASQ SOX Team, and the SOX Community was created later as the first ASQ community of interest.

The SOX team comments are intended to identify parts of the two documents that can be supported by specific quality and environmental management principles, tools and techniques. The team used the ISO 9001 and ISO 14001 standards to illustrate its comments.

The use of monitoring, measurement and data analysis to identify and correct potential risks: AS No. 5 requires company level controls that include controls to monitor the results of operations. Clauses 8.2.3 and 8.2.4 of ISO 9001 and 4.5.1 of ISO 14001 require monitoring and measurement of products and processes on a regular basis.

ISO 9001, clause 8.4, requires analysis of data generated by clauses 8.2.3 and 8.2.4 as well as customer satisfaction and supplier data. This analysis can provide information to auditors on the early identification of risks by the organization.

Maintenance of records: AS No. 5 requires the

company's ICFR to include policies and procedures pertaining to records that accurately and fairly reflect the assets of the company and provide reasonable assurance that transactions are recorded to permit ICFR.

ISO 9001, clause 4.2.4, requires that records be legible, readily identifiable and retrievable, and that a documented procedure be established to define controls needed for identification, storage, protection, retrieval, retention time and disposition of records. These controlled records can be used by external auditors.

Personnel competence: AS No. 5 discusses competence in several places. For example, it says, "The impact of the work of others on the auditor's work also depends on the relationship between the risk and the competence and objectivity of those who performed the work."

It also says, "The auditor should test the operating effectiveness of a specified control by determining whether the specified control operated as designed and whether the person performing the control possesses the necessary authority and qualifications to perform the control effectively."

ISO 9001, clause 6.2.2, and ISO 14001, clause 4.4.2, require determination of competence, provision of training and evaluation of the effectiveness of the training.

With respect to qualifications of internal quality and environmental auditors, RABQSA and ASQ provide certification of these auditors, so their work can be used by SOX auditors.

Clarification of management's roles and responsibilities: AS No. 5 requires the auditor to assess whether management's philosophy and operating style promote effective ICFR.

ISO 9001, clause 5.1 on management commitment, requires top management to provide evidence of its commitment to the development, implementation and continual improvement of the QMS.

AS No. 5 also says the auditor should test the design effectiveness of controls by ensuring that they are operated by persons with the necessary authority and competence and can prevent or detect errors or fraud.

ISO 9001, clause 5.5.1, and ISO 14001, clause 4.4.1, require top management to define responsibilities and authorities, and communicate them within the organization.

Using the work of others: AS No. 5 says that for auditing of internal control, the auditor can use the work performed by, or receive direct assistance from, internal auditors, company personnel (in addition to internal auditors), and third parties working under the direction of management or the audit committee.

AS No. 5 also says the auditor should understand the flow of transactions related to the relevant assertions, including how these transactions are initiated, authorized, processed and recorded. The auditor can perform walkthroughs to test design effectiveness. A walkthrough consists of a mix of inquiry of appropriate personnel, observation of the company's operations, inspection of relevant documentation and retesting of controls.

With respect to qualifications of internal quality and environmental auditors, RABQSA and ASQ provide certification of these auditors, so their work can be used by SOX auditors.

It is clear from these comments that robust QMSs and EMSs can provide valuable support for compliance to AS No. 5, particularly because of the standard's numerous references to using the work of others.

Team Comments on the New SEC Guidance

The SOX team also commented on the various areas of support QMSs and EMSs can provide top management in ensuring the effectiveness of a system of internal control, as covered by the SEC's guidance for reporting ICFR.

Preventive and corrective action: The guidance says management can identify preventive controls, detective controls or a combination of both, as adequately addressing financial reporting risks.

Preventive controls stop the occurrence of errors or fraud that could result in a misstatement of the financial statements, while corrective controls detect and correct errors or fraud that have already occurred.

ISO 9001, clauses 8.5.2 and 8.5.3, and ISO 14001, clause 4.5.3, provide best practices and require documented procedures for dealing with actual and potential risks, and also for taking corrective or preventive actions.

The use of monitoring, measurement and data analysis to identify and correct potential risks:

Organizations effectively using the SEC guidance should be able to satisfy the requirements of the PCAOB standard and pass the audit performed by their external auditor.

The guidance says monitoring activities must assess the quality of internal control performance over time.

ISO 9001, clauses 8.2.3 and 8.2.4, require monitoring and measurement of products and processes, and clause 8.4 requires analysis of data obtained as a result of these clauses, as well as customer satisfaction and supplier data. The results of the analysis identify risks to the organization's objectives and provide inputs to the corrective and preventive action processes.

ISO 14001, clause 4.5.1, requires monitoring and measurement of operations, and clause 4.5.2 requires evaluation of compliance to legal requirements.

Controls to manage the organization's documents and records: The guidance says management's assessment must be supported by evidence that provides reasonable support for its assessment. The nature of the evidential matter might vary based on the assessed level of ICFR risk of the underlying controls.

ISO 9001, clause 4.2, on documentation requirements, provides a method for controlling the documentation and records associated with the procedures of the organization.

Clarification of management's roles and responsibilities: The guidance says management is responsible for designing and maintaining ICFR and performing an annual evaluation that provides a reasonable basis for its assessment of whether ICFR is effective as of fiscal year-end. Management uses its knowledge of the business, its operations and processes as part of the evaluation.

ISO 9001 aligns operational compliance with financial evaluations in clauses 5.6 on management review, 8.2.2 on internal audit and 8.4 on analysis of data. ISO 14001 does this in clauses 4.6 on management review, 4.5.5 on internal audit and 4.5.2 on evaluation of compliance.

Using the work of others: The guidance notes that both the COSO framework and the Turnbull report[10] say that determining whether a system of internal control is effective is a subjective judgment resulting from an assessment of whether the five components (control environment, risk assessment, control activities, monitoring, and information and communication) are present and functioning effectively.

The quality and environmental management systems provide support for the five COSO components through compliance to ISO 9001 and ISO 14001. This support is described in detail in my *QP* September 2005 article, "Mitigate SOX Risk With ISO 9001 and 14001."[11]

Why Two Documents?

The effort by the SEC and PCAOB to refocus SOX to a risk based, top-down approach will result in organizations concentrating on the key controls that can indicate the possibility of material misstatements in financial statements.

This focus will reduce the cost of compliance, allow organizations to emphasize their important business processes and foster the use of quality improvement tools. The result will be more effective operations.

The reason there are two documents covering the same basic process is that they deal with two

different aspects of the SOX compliance effort:

1. The PCAOB standard is aimed at the external auditing process. This compliance based document provides prescriptive requirements for the auditor and the organizations being audited.
2. The principles based SEC document is nonprescriptive and defines a method for ensuring that management's system of internal control is operating effectively and is acceptable to the SEC.

Of course, there are many similarities in the two documents, and organizations effectively using the SEC guidance should be able to satisfy the requirements of the PCAOB standard and pass the audit performed by their external auditor.

The SOX team found opportunities in the two documents for building quality into the SOX compliance process. This includes the following key practices of the quality and environmental communities:

- Preventive and corrective action techniques.
- The use of monitoring, measurement and data analysis to identify and correct potential risks.
- Methodology for ensuring personnel competence.
- Controls to manage an organization's documentation and records.
- Clarification of management's roles and responsibilities.
- The use of the work of QMS and EMS personnel in a SOX audit.

The bottom line is that QMSs and EMSs and the involved personnel can support financial management in compliance to SOX. This was made clear in the SOX team's full set of comments to the SEC and PCAOB.

REFERENCES AND NOTES

1. The Corporate and Criminal Fraud Accountability Act of 2002, also known as the Sarbanes-Oxley Act (Public Law 107-204), U.S. Congress, 2002; see the frequently asked questions at www.asq.org/communities/sarbanes-oxley/faq.html for a link to a copy of the law.

2. *Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AS No. 2), PCAOB, 2004.

3. Public Company Accounting Oversight Board, PCAOB Release No. 2006-007, PCAOB Rulemaking Docket Matter No. 021, *Proposed Auditing Standard—An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements and Related Other Proposals*, 2006, www.asq.org/communities/sarbanes-oxley/abstracts/team-comments.html

4. Securities and Exchange Commission, File No. S7-24-06, *Management's Report on Internal Control Over Financial Reporting*, 2006, www.asq.org/communities/sarbanes-oxley/abstracts/team-comments.html

5. Letters dated Feb. 23, 2007, www.asq.org/communities/sarbanes-oxley/abstracts/team-comments.html.

6. Public Company Accounting Oversight Board, PCAOB Release No. 2007-005, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements and Related Independence Rule and Conforming Amendments*, 2007.

7. Securities and Exchange Commission, 17 CFR Part 241, *Commission Guide Regarding Management's Report on Internal Control Over Financial Reporting*, 2007.

8. COSO, "Internal Control—Integrated Framework," 1992. This is commonly called the COSO guidance.

9. The four team members were Sandford Liebesman, Paul Palmes, John Walz and Donna Spencer. Marty Jaeger and Chad Kymal joined the team later.

10. *Internal Control, Guidance for Directors on the Combined Code*, Institute of Chartered Accountants in England and Wales, 1999.

11. Sandford Liebesman, "Mitigate SOX Risk With ISO 9001 and 14001," *Quality Progress*, September 2005, pp. 91-93.

SANDFORD LIEBESMAN *had more than 30 years of experience in quality at Bell Laboratories, Lucent Technologies and Bellcore (Telcordia) before becoming a consultant. He is an ISO 9000 subject matter expert and author of the books* TL 9000, Release 3.0: A Guide to Measuring Excellence in Telecommunications, *second edition, and* Using ISO 9000 to Improve Business Processes. *He is a member of ISO technical committee 176 and the ANSI Z-1 committee on quality assurance. Liebesman is certified by the RABQSA International as an ISO 9000 and TL 9000 lead auditor. He is an ASQ fellow.*

Please comment

If you would like to comment on this article, please post your remarks on the *Quality Progress* Discussion Board at www.asq.org, or e-mail them to editor@asq.org.